UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,165	10/31/2003	**Jonathan D. Herbach**	07844-623001	1607

21876 7590 06/03/2010

FISH & RICHARDSON P.C.
P.O. Box 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
DUNN, DARRIN D	

ART UNIT	PAPER NUMBER
2121	

NOTIFICATION DATE	DELIVERY MODE
06/03/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No.	Applicant(s)	
	10/699,165	HERBACH ET AL.	
	Examiner	Art Unit	
	DARRIN DUNN	2121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 February 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,23-29 and 35-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8, 23-29, and 35-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/23/10*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☒ Other: *Provisional Patents attached ('810, '388, '626)* .

DETAILED ACTION

1. The Office Action is responsive to the communication filed on 2/23/10.

2. Claims 1-8, 23-29, and 35-41 are pending in the application.

Response to Amendment

3. The amendment, filed 02/23/10, has been entered. The U.S.C section 112 rejection has been removed.

Response to Arguments

4. Applicant's arguments filed 02/23/10 have been fully considered but they are not persuasive.

A] Applicant states that as an initial issue the non-provisional application, Raciborski (USPN 2005/0132083, contains subject matter that is not supported by provisional applications 60/490810, 60/500388, and 60508626. Applicant further states that the Office has not provided evidence that the subject matter relied on by Raciborski is also presented in the priority documents. In response, evidence of the subject matter has been provided. Please reference the enclosed copies of the aforementioned priority documents for supporting subject matter, see attachments 60490810, 60500388, and 60508626.

B] Applicant states that MacInnis explicitly discourages using a client initiated request because selectively downloading software and data modules to terminals in a network does not require communication between the terminal and the downloading source ([0011]). When read in light

of the context of the disclosure, downloading schemes presented in certain networks such as television subscription systems introduces a two way communication system that is expensive and difficult to provide ([0007]). Although it is agreed that in certain types of networks, there is no motivation to provide two way communications, it is recognized that two way communications is necessary in other types of networks. As modified, the pertinent problem of downloading source versions based on client capabilities, as per MacInnis, is applied to a network presented in Raciborski. This network involves two way communications between a client and a source for downloading content objects via user requests. Although the field of endeavor in MacInnis, as applied to television subscription systems, avoids implementing two way communications, a skilled artisan would appreciate the applicability of the download scheme presented in MacInnis is applicable to networks configured to support content object download requests. In effect, the motivation to apply the download schema, as per [0011], is based upon solving the pertinent problem of ensuring software is compatible with client capabilities in light of networks configured to facilitate software downloads.

C] Applicant states that claim 1 is clearly directed to providing an appropriate program to a client to authenticate a user based on a document being accessed by the user and the action requested with respect to the document. Applicant argues that the references cited do not control access to a document by sending information specifying an acceptable authentication procedure after determining whether user authentication is needed based on the document identifier and the action.

The Examiner respectfully disagrees. Raciborski teaches accessing a document by a user ([0028] e.g., any number if user computers may download one or more content objects over the internet). In response, user authentication is needed based on the document identifier and the action (e.g., as interpreted, a user requesting a document for download is verified, such as ensuring the user purchased the contents prior to download ([0020]. Also, for content previously purchased, the media server can later allow download by checking authorization in the user information database ([0030]) Subsequently, a download manager is compiled after the content objects are requested ....there can be different versions of the download manager software ([0033]). The user can execute the download manager program after download ([0036]) In effect, in response to the user selecting a content object (e.g., identifier such as audio, video) for download (action), a download manager implementing a password interface is downloaded ([0037]) (e.g., authentication procedure). Upon a successful download of the manager, as modified, it is obvious that this program may become outdated. In response, a client will request an updated version for the download manager software but only after processing the information specifying an acceptable authentication procedure (e.g., best program for download), supra page 4, prior office action (e.g., receiving an updated authentication procedure update request from the client in response to client processing of the information specifying an acceptable authentication procedure)

Applicant has not defined the following terms:

- Information is not defined.

-Authentication procedure is not defined

D] The Examiner agrees that the applicant has tied together the claim elements.

E] Suggested Clarifications:

The download manager is compiled per content object so as to be unique and one type. In contrast, applicant's authentication program may be unique per content type requested.

The download manager itself is updated for the purpose of maintaining compatibility and a current state. In contrast, applicant's request is not limited to the purpose of updating the existing software. Rather, the update request, as understood, is configured to retrieve multiple types of authentication programs for the user based upon an action and content type.

Also, unless otherwise mistaken, an authentication procedure may be encapsulated as a module that is a sub-part of an authentication program. The module itself may be downloaded as part of the update request so as to enable a client to present various authentication types(e.g., bio-metric, login box, retinal scan, etc)

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 1,3-4, 6-7, 23, 25, 28, 36-37, 39-40 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Raciborski et al. (USPN 20050132083) in view over MacInnis (USPN 20030028899).

8. As per claim 1, Raciborski et al. teaches a method comprising:

receiving, at a server, a request from a client to take an action with respect to an electronic document ([ABSTRACT], [0028])

retrieving a document identifier (e.g., content object descriptions) from the request ([0028], [0032]);

determining whether user authentication is needed based on the document identifier and the action ([0020], [0030] [0035], [0036] e.g., authorization is performed, i.e., checking rights for purchased content, based on the content object and making use of the content object)

Raciborski et al. teaches a specified authentication procedure ([0033] e.g., an authentication procedure is interpreted as a program that uses authentication steps. The program corresponds to the download manager. The download manager software uses an authentication procedure, i.e., password interface, to verify the user is permitted to access the content objects ([0037])

Raciborski et al. is silent as to sending information specifying an acceptable authentication procedure. For clarity, multiple versions of the download manager will be discussed below. The manager program is considered an acceptable authentication procedure. However, it is foreseeable that multiple versions may be present on the server, which may result in

compatibility issues with the client. Therefore, there is a need to send information regarding the most suitable version of the download manager, i.e., authentication procedure, that the client should be using)

MacInnis teaches sending information specifying an acceptable authentication procedure ([ABSTRACT], [0012] e.g., descriptor information, i.e., information regarding an acceptable procedure. The Examiner's position is that a) a download manager is compiled and available to a client and b) before downloading a particular manager, descriptive information is provided to the client such that the best 'module version,' i.e., download manager, is available to the client. This version of the download manager provides an authentication procedure, i.e., checking user restrictions when downloading content objects, see [0045], [0039])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Raciborski et al. to include descriptor information sent to the client such that the client could choose the 'best' manager program, as taught by MacInnis. Raciborski et al. teaches multiple, available versions of a download manager ([0033]). MacInnis teaches enabling the client to select the best 'module version.' Since enabling the client to select the best and most often compatible version of the download manager, i.e., authentication procedure, based on client capabilities, it would have been obvious to send descriptive information about the manager program, i.e., authentication procedure, to ensure a compatible program |program version is downloaded and installed)

MacInnis teaches receiving an authentication procedure update request ([0012] e.g., it is interpreted that as authoring sources generate module versions, new versions become available to the client. A client would select a new version of the download manager, i.e., authentication

procedure update request) in response to the client processing of the information specifying an acceptable authentication procedure (e.g., when new versions are available, the client could review and install these versions after receiving the descriptor list, i.e., processing information. After processing the information, the client could request the new version, i.e., authentication procedure update) but does not teach the request for information, i.e., descriptors, is initiated by the client. MacInnis teaches a client initiating the request for updates ([0007] e.g., the Examiner's position the aforementioned steps could be initiated by the client simply by communicating a need for updates to the server. From this point, the server would then send the client the descriptor list)

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to enable a client to request an updated procedure. MacInnis teaches that new versions are made available to the client, which would be unknown to the client. MacInnis, as modified, teaches that a client would make a request for new versions. MacInnis, as modified, teaches that in response a descriptor list would be sent to the client showing the client the available versions, and from which a client may select the best version. In effect, in response to the client processing the available list, i.e., information specifying an acceptable authentication procedure, the client would receive an updated version of a program.

Raciborski et al teaches obtaining, at the server and in response to the authentication procedure update request (e.g., client requesting a new version of the download manager, where this manager includes authentication steps), a software program (e.g., download manager) comprising instructions operable to cause one or more data processing apparatus to perform operations effecting the authentication procedure ([0033] e.g., a download manager, i.e.,

software program, embodies authentication step such as checking user authentication, i.e., steps to authenticate a user); and

sending the software program to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document ([0032], [0033], [0035] e.g., downloading manager software)

9. As per claim 3, teaches receiving, at a se Raciborski et al. teaches a method comprising:

receiving, at a server, a request from a client to take an action with respect to an electronic document ([ABSTRACT], [0028], [0032])

obtaining, at the server and in response to the request, a software program (e.g., download manager embodying an authentication procedure) comprising instructions operable to cause one or more data processing apparatus to perform operations effecting the authentication procedure ([0033] e.g., a download manager, i.e., software program, is selected as the best module available in response to the client processing descriptor lists, i.e., information specifying an acceptable authentication procedure. The download manager effectuates an authentication procedure, i.e., verifying the user ([0037])

sending the software program to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document ([0032], [0033], [0035], [0037] e.g., downloading manager program. The user is identified [0037]. Based on user authentication, content objects are accessible);

receiving an updated authentication procedure (e.g., Raciborski et al. as modified by MacInnis, teaches where the program would have authoring sources generating new modules ([0012] e.g., updated authentication procedure or updating the download manager. It is interpreted that a new version, as generated, is an updated authentication procedure because a download program is a procedure to authenticate a user)

receiving a subsequent request from the client to take the action with respect to the electronic document (e.g., as modified, supra claim 1, a client would make a request for a newer version. This solves the pertinent problem of ensuring that the client is always up to date);

obtaining, at the server and in response to the subsequent request, a new software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting the updated authentication procedure (e.g., supra claim 1, where a new version is made available, the client receives the available versions prior to downloading (e.g., descriptor list), and subsequently the client would install the new program. The Examiner's position is that as new modules become available, a client could initiate a check to see whether a new module is available, in response the client would receive a descriptor list showing the available versions, and in response select the best module);

sending the new software program to the client for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document-permissions information associated with the electronic document ([0033] e.g., as modified, supra claim 1 discussion, new versions are made available, i.e., new software program, for subsequent installation)

10. As per claim 23, Raciborski et al., as modified, teaches a system comprising:

a client that sends an authentication procedure update request (e.g., requesting new version of the download manager) to a server in response to client processing of information received from the server (e.g., supra claim 1 discussion. In response to the client processing available versions, i.e., descriptor list, the client would request a newer version of software based on the received descriptor list. The initial request could be initiated by the client such that following the request for newer versions, the client would process the descriptor list, and then request a newer version. The initial client request is simply for checking for new versions. Following this initial request, the client can request an actual version, i.e., requesting authentication procedure update based on the received descriptor list)

wherein the information received from the server specifies one or more acceptable authentication procedures (e.g., descriptor list. As modified, the descriptor list would include the available versions of a download manager)

the server that receives the authentication procedure update request, and in response to the client, the server obtains and sends a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure (e.g., supra claim 1, where the server has multiple versions of modules, in response to the client needing software, the server sends the descriptor list to the client, the client can then make a request for a new version of software, and the server will send the software to the client); and

wherein the client uses the software program (e.g., download manager) to identify the current user (0037) and control an action with respect to an electronic document based on the current user and document-permissions information associated with the electronic document, and

wherein the action comprises an action taken with respect to the electronic document subsequent to opening the electronic document at the client ([0043], [Figure 4D] e.g., supra claim 1 discussion)

11. As per claim 25 Rociborski et al. teaches the system of claim 23, wherein the client includes a security handler that provides a server-communication interface to the software program ([0020] e.g., transaction session identifier)

12. As per claim 36, teaches the system of claim 23, Raciborski et al., as modified, teaches wherein the server receives a subsequent request from the client to take action with respect to the electronic document ([0045] e.g., downloads implies that more than one request can be made) but Raciborski et al. does not teach obtaining, in response to the subsequent request, a new authentication process, and sends the new authentication process to the client for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document permissions information associated with the electronic document. MacInnis teaches checking for new versions and enabling the client to continuously be updated with versions

Therefore, it would have been obvious to one of ordinary skill in the art to have provided a client with an updated authentication program if a newer version was available at the time of communication. It is foreseeable that newer versions are made available, these versions may be made available in response to a client seeking an update, a server informing the client of an update, and or when a client communicates with the server (e.g., as in the case of requesting downloads).

13. As per claims 4 and 37, Raciborski et al. teaches software program uses an existing interface provided by the client to communicate authentication information to the server ([FIG 2A-208])

14. Claims 5, 26, and 38 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Raciborski et al. (USPN 20050132083) in view over MacInnis (USPN 20030028899) and in further view over Hu (USPN 5586260)

15. As per claims 5, 26, and 38, Raciborski et al. teaches receiving credentials information from the client derived at least in part based on input obtained by the client using the software program ([0041], [0043] e.g., passwords) but does not teach communicating with a third part authentication server to authenticate the current user based on the credentials information. Hu teaches a third party authentication server ([ABSTRACT])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to implement a third party authentication server as taught by Hu et al. Hu teaches a method for authenticating a client for a server. Raciborski teaches a system for authenticating a user/client to enable access to content stored on a server. Since a third party authentication server provides a well known means in which to maintain, store, and retrieve credentials, it would have been advantageous to provide this server as an additional means, in effect providing both redundancy in addition to reducing load on the primary server.

16. As per claims 6 and 39 Rociborski et al. teaches the method of claim 5, wherein the input obtained by the client comprises text input ([0041], [0043] e.g., password).

17. As per claims 7 and 40, Rociborski et al. teaches the method of claim 5, wherein the input obtained by the client comprises biometric data ([0043] e.g., biometric authentication)

18. Claims 8, 27, 38, and 41 are rejected over Raciborski et al. (USPN 20050132083) in view of Heath et al. (USPN 6006034) and in further view of Hu (USPN 5586260).

19. As per claims 8,27, 38, and 41, Raciborski et al. teaches receiving input from a client using the software ([0041], [0043]) e.g., password). It does not teach receiving an authentication receipt from a third party authentication server based on input obtained by the client using the software. Hu teaches returning an access key from an authentication gateway acting as a proxy server to the client, i.e., receipt, based on credentials ([ABSTRACT], [COL 1 lines 58-63] e.g., receiving an authentication receipt from a third party authentication server) and verifying the current user with the third party authentication server using the authentication receipt ([COL 1 lines 18-20], lines 59-63], [ABSTRACT] e.g., authenticating a client)

Therefore, at the time the invention was made, it would have been obvious to have provided a means in which to authenticate a client via saving security credentials,. Raciborski et al. teaches authenticating a user via credentials as to enable access to content on a server. Hu et al. teaches saving security credentials for later use and generating an access key for their retrieval and passing the access key to the client. In effect, saving the security credentials for later use and providing an access key for their retrieval obviates the need for repeated authentication. As a result, the system is further optimized and limits redundant authentication procedures.

20. As per claim 28, Raciborski et al., as modified, teaches a server comprising:

a server core with configuration and logging components ([0029])

an internal services component that provides functionality across dynamically loaded methods ([0029] e.g., web page)

dynamically loaded external services providers, including an authentication service provide (supra Hu for authentication server - ABSTRACT)

21. Claim 29 is rejected under 35 U.S.C. 103 (a) as being unpatentable over Raciborski et al. (USPN 20050132083) in view over MacInnis (USPN 20030028899) and in further view over Tenerelllo (USPN 7233981)

22. As per claim 29, Raciborski et al. teaches a business logic tier comprising a cluster of document control servers ([0029] e.g. content delivery networks); an application tier including the client comprising a viewer client, a securing client, and an administration client ([FIG 1-FIG 2A – client computer functions via providing a view – browser, securing – downloading the manager (securing a program), and administration (storage media)). However, Racoborski et al. does not teach a load balancer that routes client requests to the document control server. Tenerello teaches a system and method for load balancing ([COL 1 lines 14-20], [COL 2 lines 63-67])

Therefore, at the time the invention was made, one of ordinary skill would have motivation to load balance a system. Raciborski et al. teaches that various user computers may access content objects ([0029]) Tenerello teaches a load balancing means in which multiple requests may be efficiently processed. Since load balancing increases performance of a system, it would have been obvious to have enabled a system employing multiple user computers, each requesting access to a resource, a means to load balance the requests as to optimize the system.

23. Claims 2, 24, and 35 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Raciborski et al. (USPN 20050132083) in view over MacInnis (USPN 20030028899) and in further view over Kano et al. (USPN 20030135650)

24. As per claims 2, 24, and 35, Raciborski et al. does not teach a second server providing the software program. Kano et al. teaches a backup server ([ABSTRACT])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to include a backup server as a means of providing redundancy. In the event of a failure of the primary server, it would have been beneficial to utilize a backup server as a means of distributing the software program, modules, and versions as they become available.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARRIN DUNN whose telephone number is (571)270-1645. The examiner can normally be reached on EST:M-R(8:00-5:00) 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DD/
05/22/10

/Albert DeCady/
Supervisory Patent Examiner
Art Unit 2121